Module 2 | Architecture & Analysis

Introduction

This module looks at big picture issues with respect to campaign development and defense to frame the technical details we'll be learning over the next few modules. We will look over the types of malware campaigns you'll encounter today, how to analyze systems from an attacker's perspective, and ways you can organize attack and defense activities.

Learning Objectives

The primary class objectives we address in this module is to be able to *Explain the different types of malware campaigns* and to *defensively and offensively analyze a system*.

All homework should be completed and initially submitted by the end of this module, which you should complete by the end of the second week. The homework assignment associated with this module is a report designing how you would attack an internet camera in my office.

Required Instructional Materials

All you'll need for this section are the video lectures and the tooling we cover. That said, you will likely want to refer to external documentation and tutorials on the Python programming environment. You'll need an internet connection to access, install, and read about the tools we cover.

This module is much meatier than the previous. I suggest you start as soon as you can and front load your schedule by getting as much done as early in the week as possible. The homework assignment associated with this module is at the end of the module and requires you to have looked over the module material, and you'll want to have as much time as possible for that.

Summary

- This module consists of a series of video lectures. We reference a variety of tools and external sites and documentation you'll likely want to review.
- This module has an associated module project. You'll want to view all the videos and be familiar with the material prior to starting, but it's not a bad idea to take a look at it early so you have something to frame what you should learn in this module.